Amendments to the Claims:

The following listing of claims will replace all prior versions of the claims in the application.

1. (Currently Amended) A data optimization engine disposed inline with a first communication channel and a second communication channel, comprising:

a transmit interface circuit configured to receive a first data stream from said first communication channel and to obtain [a] first data [file] from said first data stream; and

an optimization processor coupled to said transmit interface circuit for receiving [a] second data [file] from said transmit interface circuit, said second data [file] representing said first data [file] after said first data [file] has been processed by said transmit interface circuit into a format suitable for optimization by said optimization processor, said optimization processor being configured to ascertain whether said second data is compressible and whether said second data is a candidate for encryption, said optimization processor being configured to perform in the alternative one of four actions with respect to said second data, a first action of said four actions involving compressing said second data to form compressed data and encrypting said compressed data if said second data is ascertained to be both compressible and said candidate for encryption, a second action of said four actions involving compressing said second data without encrypting said second data if said second data is ascertained to be compressible but not said candidate for encryption, a third action of said four actions involving encrypting said second data without compressing said second data if said second data is ascertained to be not compressible but is ascertained to be said candidate for encryption, a fourth action of said four actions involving neither encrypting nor compressing said second data if said second data is ascertained to be not compressible and not said candidate for encryption. [performs one of a compression and an encryption on said second data file, thereby obtaining an optimized data file.]

2. (Original) The data optimization engine of claim 1 wherein said first data [file] is a Fiber Channel data frame.

3. (Original) The data optimization engine of claim 2 wherein said first data [file] is encoded using 10-bit encoding, said format suitable for optimization by said optimization processor is an 8-bit encoding protocol.

4. (Currently Amended) The data optimization engine of claim 1 further including a receive interface circuit coupled to said optimization processor, said receive interface circuit being configured to receive a second data stream from said second communication channel and to obtain [a]third data [file] from said second data stream, said third data [file] representing a data [file] previously optimized and requiring deoptimization, said receive interface circuit also being configured to send [a]fourth data [file] to said optimization processor, said fourth data [file] representing said third data [file] after said third data [file] has been processed by said receive interface circuit into a format suitable for deoptimization by said optimization processor, said optimization processor being configured to ascertain whether said fourth data is previously compressed and whether said fourth data is a candidate for decryption, said optimization processor being configured to perform in the alternative one of four actions with respect to said fourth data, a first action of said four actions involving decompressing said fourth data to form decompressed data and decrypting said decompressed data if said fourth data is ascertained to be both previously compressed and said candidate for decryption, a second action of said four actions involving decompressing said fourth data without decrypting said fourth data if said fourth data is ascertained to be previously compressed but not said candidate for decryption, a third action of said four actions involving decrypting said fourth data without decompressing said fourth data if said fourth data is ascertained to be not previously compressed but is ascertained to be said candidate for decryption, a fourth action of said four actions involving neither decrypting nor decompressing said fourth data if said fourth data is ascertained to be not previously compressed and not said candidate for decryption. [performs one of a decompression and a decryption on said fourth data file, thereby obtaining a deoptimized data file.]

5. (New) The data optimization engine of claim 4 wherein said encryption involves public key encryption.

6. (New) The data optimization engine of claim 4 wherein said optimization processor ascertains whether said second data is compressible by examining a header field associated with said second data.

7. (New) The data optimization engine of claim 4 wherein said optimization processor ascertains whether said second data is said candidate for encryption by examining a header field associated with said second data.

8. (New) The data optimization engine of claim 4 wherein said optimization processor ascertains whether said second data is said candidate for encryption by detecting a presence of an encryption key.

9. (New) The data optimization engine of claim 4 wherein said third data is obtained responsive to a memory read (MR) operation.

10. (New) The data optimization engine of claim 4 wherein said third data is obtained responsive to a request to read data from a storage device.

11. (New) The data optimization engine of claim 1 wherein said first communication channel is associated with a Fiber Channel Controller.

12. (New) The data optimization engine of claim 1 wherein said first communication channel is associated with a SERDES.

13. (New) The data optimization engine of claim 1 wherein said first communication channel is coupled with a first PCI device, said second communication channel is coupled with a second PCI device.

14. (New) The data optimization engine of claim 1 wherein said first communication channel is coupled with a first network device, said second communication channel is coupled with a second network device.

15. (New) The data optimization engine of claim 14 wherein said first network device represents one of a network interface card, a router, and a switch.

16. (New) The data optimization engine of claim 1 wherein said second data is associated with a memory write (MW) operation involving a computer system memory.

17. (New) The data optimization engine of claim 1 wherein said first data is received from a CPU of a computer system, output data from said optimization processor being destined for storage in memory of said computer system.

18. (New) The data optimization engine of claim 1 further comprising

a compression engine for performing said encrypting if said second data is ascertained to be compressible; and

a packer coupled to output of said compression engine, said packer being configured to pack data output from said compression engine into a continuous stream in groups of n, whereby n represents the number of bits required by interface circuitry employed for transmitting on said second communication channel.

19. (New) The data optimization engine of claim 1 wherein said optimization processor is further configured to ascertain whether said first data represents data associated with a control

transaction, said first data is permitted to bypass said optimization engine if said first data represents said data associated with said control transaction.

20. (New) A data optimization engine disposed inline with a first communication channel and a second communication channel, comprising:

an optimization processor configured to ascertain whether first data received via said first communication channel is compressible and whether said first data is a candidate for encryption, said optimization processor being configured to perform in the alternative one of four actions with respect to said first data, a first action of said four actions involving compressing said first data to form compressed data and encrypting said compressed data if said first data is ascertained to be both compressible and said candidate for encryption, a second action of said four actions involving compressing said first data without encrypting said first data if said first data is ascertained to be compressible but not said candidate for encryption, a third action of said four actions involving encrypting said first data without compressing said first data if said first data is ascertained to be not compressible but is ascertained to be said candidate for encryption, a fourth action of said four actions involving neither encrypting nor compressing said first data if said first data is ascertained to be not compressible and not said candidate for encryption.

21. (New) The data optimization engine of claim 20 wherein said encryption involves public key encryption.

22. (New) The data optimization engine of claim 20 wherein said optimization processor ascertains whether said first data is compressible by examining a header field associated with said first data.

23. (New) The data optimization engine of claim 20 wherein said optimization processor ascertains whether said first data is said candidate for encryption by examining a header field associated with said first data.

24. (New) The data optimization engine of claim 20 wherein said optimization processor ascertains whether said first data is said candidate for encryption by detecting a presence of an encryption key.

25. (New) A method for performing inline optimization of data using a data optimization engine disposed inline with a first communication channel and a second communication channel, comprising:

ascertaining whether first data received via said first communication channel is compressible;

ascertaining whether said first data is a candidate for encryption; and

performing, using said optimization processor, in the alternative one of four actions with respect to said first data, a first action of said four actions involving compressing said first data to form compressed data and encrypting said compressed data if said first data is ascertained to be both compressible and said candidate for encryption, a second action of said four actions involving compressing said first data without encrypting said first data if said first data is ascertained to be compressible but not said candidate for encryption, a third action of said four actions involving encrypting said first data without compressing said first data if said first data is ascertained to be not compressible but is ascertained to be said candidate for encryption, a fourth action of said four actions involving neither encrypting nor compressing said first data if said first data is ascertained to be not compressible and not said candidate for encryption.

26. (New) The method of claim 25 wherein said encryption involves public key encryption.

27. (New) The method of claim 25 wherein said ascertaining whether said first data is compressible includes examining a header field associated with said first data.

28. (New) The method of claim 25 wherein said ascertaining whether said first data is said candidate for encryption includes examining a header field associated with said first data.

29. (New) The method of claim 25 wherein said ascertaining whether said first data is said candidate for encryption includes detecting a presence of an encryption key.